Bounds on Key Appearance Equivocation for Substitution Ciphers

Yuri Borissov and Moon Ho Lee, *Senior Member, IEEE*

Abstract— **The average conditional entropy of the key given the message and its corresponding cryptogram, $H(\mathbf{K}|\mathbf{M}, \mathbf{C})$, which is reffer as a key appearance equivocation, was proposed as a theoretical measure of the strength of the cipher system under a known-plaintext attack by Dunham in 1980. In the same work (among other things), lower and upper bounds for $H(\mathcal{S}_{\mathcal{M}}|\mathbf{M}^L\mathbf{C}^L)$ are found and its asymptotic behaviour as a function of cryptogram length L is described for simple substitution ciphers i.e. when the key space $\mathcal{S}_{\mathcal{M}}$ is the symmetric group acting on a discrete alphabet $\mathcal{M}$. In the present paper we consider the same problem when the key space is an arbitrary subgroup $\mathcal{K} \lhd \mathcal{S}_{\mathcal{M}}$ and generalize Dunham's result.**

Index Terms— **key appearance equivocation, substituion ciphers.**

I. Introduction

Shannon in his seminal paper [2] showed that the conditional entropies of the key and message given the cryptogram can be used as a theoretical measure of strength of the cipher system when assuming unlimited cryptanalytic computational capabilities. These conditional entropies are called the key and message equivocation, respectively.

In general it is diffucult to calculate these equivocations explicitly. For that Shannon established in [2] a general lower bound and introduced a random cipher model which would approximate the behaviour of complex practical ciphers. Afterward, Hellman [3] reviewed and extended Shannon's information-theoretic approach and showed that random cipher model is conservative in that a randomly chosen cipher is essentially the worst possible. Later on Blom [4] obtained exponentially tight bounds on the key equivocation for simple substitution ciphers. In [1] to derive bounds for simple substitution ciphers on the message equivocation in terms of the key equivocation, Dunham derived such bounds for so-called key appearance equivocation. This author pointed out also, that it can be considered as a theoretical measure of the strength of the cipher system under known-plaintext attack. Another contribution of this subject is the Sgarro's work [5].

In Section II we give the necessary background and state a theorem which gives the bounds on the key appearance equivocation for substitution ciphers when the key space is confined to a subgroup $\mathcal{K}$ of the group $\mathcal{S}_{\mathcal{M}}$ of all substitutions of a discrete alphabet $\mathcal{M}$. In Section III we discuss four applications of the stated theorem in some particular cases. Finally, we conclude in Section IV.

Yuri Borissov is with the Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia 1113, Bulgaria. Moon Ho Lee is with the Institute of Information and Communication, Chonbuk National University, Jeonju 561-756, R. Korea.

II. Lower and Upper Bounds for the Key Appearance Equivocation

For basic definitions and notions we reffer to [2],[1] and [6]. Let a memoryless message source with a discrete finite alphabet $\mathcal{M} = \{1, 2, \ldots, N\}$ be given. The probability of a symbol n is denoted by $P_{\mathcal{M}}(n)$. The cryptogram alphabet $\mathcal{C}$ is taken to be the same as $\mathcal{M}$, and the key space is $\mathcal{K} \lhd \mathcal{S}_{\mathcal{M}}$ – an arbitrary subgroup of the the symmetric group acting on $\mathcal{M}$. For every $\pi \in \mathcal{K}$ the cryptographic transformation $\mathrm{T}_{\pi} : \mathcal{M}^L \to \mathcal{M}^L$ is determined in the following way: If $\mathbf{m}^L = m_1 m_2 \ldots m_L$ is a message of length L, then the cryptogram is $\mathbf{c}^L = \mathrm{T}_{\pi}(\mathbf{m}^L) \stackrel{\text{def}}{=} \pi(m_1)\pi(m_2)\ldots\pi(m_L)$. We assume also that the key and message sources are independent, and the keys are equiprobable, i.e. $P_{\mathcal{K}}(\pi) = 1/|\mathcal{K}|$.

We make use of the following lemma:

Lemma 2.1: Let G be a group of substitutions of the finite set X. If the set $G(i, j) = \{\pi \in G/\pi(i) = j\}$, where i and j are some fixed elements of X, is nonempty, then it is a left coset by the stabilizer $St(i) \stackrel{\text{def}}{=} \{\tau \in G/\tau(i) = i\}$.

Proof: Obviously, if $\pi(i) \in G(i, j)$ then for any $\alpha \in St(i)$ we have $\pi \circ \alpha(i) = \pi(i) = j$. Conversely, if $\pi(i) = j$ and $\tau(i) = j$ then $\pi^{-1} \circ \tau(i) = \pi^{-1}(j) = i$ hence $\pi^{-1} \circ \tau \in St(i)$. ∎

In order to state the main theorem we need the following definitions:

DEFINITION 2.2: The set $F(\pi) \stackrel{\text{def}}{=} \{j/\pi(j) = j\}$ is called a fixed set of $\pi \in \mathcal{K}$.

Let us denote by $\mathcal{K}^*$ the set of all substitutions in $\mathcal{K}$ excluding the identity.

DEFINITION 2.3: The key $\pi \in \mathcal{K}^*$ is called maximal when its fixed set $F(\pi)$ is maximal in sense of inclusion among the sets $F(\tau)$, $\tau \in \mathcal{K}^*$.

We will denote by $\mathcal{K}_{\max}$ the set of all maximal keys and for any $\pi \in \mathcal{K}_{\max}$ by P_{π} the sum of probablities $\sum_{j \in F(\pi)} P_{\mathcal{M}}(j)$.

For completeness of exposition we recall the defintion of key appearance equivocation:

DEFINITION 2.4:

$$H(\mathbf{K}|\mathbf{M}^L\mathbf{C}^L) \stackrel{\text{def}}{=} \sum_{\mathbf{m}^L \in \mathbf{M}^L} \sum_{\mathbf{c}^L \in \mathbf{C}^L} H(\mathbf{K}|\mathbf{m}^L\mathbf{c}^L) P_{\mathcal{M}^L\mathcal{C}^L}(\mathbf{m}^L\mathbf{c}^L)$$

and

$$H(\mathbf{K}|\mathbf{m}^L\mathbf{c}^L) \stackrel{\text{def}}{=} \sum_{k:\mathrm{T}_{\mathrm{k}}(\mathbf{m}^L)=\mathbf{c}^L} P_{\mathbf{K}}(k) log(1/P_{\mathbf{K}}(k))$$

The following theorem is a generalization of the result obtained in [1] on the behaviour of key appearance equivocation for simple substitution ciphers as a function of cryptogram length.

Theorem 2.5: Under the above impossed assumptions, let $\mathcal{K}_{\max}$ is nonempty and $R = \max\{P_\tau/\tau \in \mathcal{K}_{\max}\}$. Then the following inequalities hold:

$$\log(2)R^L \leq H(\mathcal{K}|\mathbf{M}^L\mathbf{C}^L) \leq \log(|\mathcal{K}|)|\mathcal{K}_{\max}|R^L$$

Remark. The logarithms are taken for an arbitrary fixed base depending on the unit of entropy measurement.

Proof: Starting from definition of conditional entropy, using the fact that the keys are equiprobable and applying Lemma 2.1 we consecutively get:

$$\sum_{\mathbf{m}^L \in \mathbf{M}^L\mathbf{c}^L \in \mathbf{C}^L} H(\mathbf{K}|\mathbf{m}^L\mathbf{c}^L)P_{\mathcal{M}^L\mathcal{C}^L}(\mathbf{m}^L\mathbf{c}^L) =$$

$$\sum_{\mathbf{m}^L \in \mathbf{M}^L\mathbf{c}^L \in \mathbf{C}^L} log(|St(\mathbf{m}^L)|)P_{\mathcal{M}^L\mathcal{C}^L}(\mathbf{m}^L\mathbf{c}^L) =$$

$$\sum_{\mathbf{m}^L \in \mathbf{M}^L} log(|St(\mathbf{m}^L)|) \sum_{\mathbf{c}^L \in \mathbf{C}^L} P_{\mathcal{M}^L\mathcal{C}^L}(\mathbf{m}^L\mathbf{c}^L) =$$

$$\sum_{\mathbf{m}^L \in \mathbf{M}^L} log(|St(\mathbf{m}^L)|)P_{\mathcal{M}^L}(\mathbf{m}^L),$$

where $St(\mathbf{m}^L) = \{T_\pi/T_\pi(\mathbf{m}^L) = \mathbf{m}^L, \pi \in \mathcal{K}\}$ is the stabilizer of message $\mathbf{m}^L$.

Clearly, if $St(\mathbf{m}^L) \neq \{e\}$, where e is identity, we have: $2 \leq |St(\mathbf{m}^L)| \leq |\mathcal{K}|$. Thus the following inequalities hold:

$$log(2) \sum_{\mathbf{m}^L:St(\mathbf{m}^L)\neq\{e\}} P_{\mathcal{M}^L}(\mathbf{m}^L) \leq H(\mathcal{K}|\mathbf{M}^L\mathbf{C}^L) \leq$$

$$log(|\mathcal{K}|) \sum_{\mathbf{m}^L:St(\mathbf{m}^L)\neq\{e\}} P_{\mathcal{M}^L}(\mathbf{m}^L) \qquad (1)$$

The fact that the message source is memoryless implies for any $\Omega \subset \mathcal{M}$ and $(m_1m_2\ldots m_L) = \mathbf{m}^L \in \Omega^L$

$$\sum_{\mathbf{m}^L} P_{\mathcal{M}^L}(\mathbf{m}^L) = \sum_{\mathbf{m}^L} \prod_{l=1}^{L} P_{\mathcal{M}}(m_l)$$

$$= (\sum_{m \in \Omega} P_{\mathcal{M}}(m))^L$$

Let $R = P_\pi$. Since $T_\pi \in St(\mathbf{m}^L)$ for any $\mathbf{m}^L \in [F(\pi)]^L$ then $[F(\pi)]^L \subset \{\mathbf{m}^L \in \mathcal{M}^L/St(\mathbf{m}^L) \neq \{e\}\}$. Therefore the following inequality holds:

$$R^L = (\sum_{m \in F(\pi)} P_{\mathcal{M}}(m))^L = \sum_{\mathbf{m}^L \in [F(\pi)]^L} P_{\mathcal{M}^L}(\mathbf{m}^L) \leq$$

$$\sum_{\mathbf{m}^L:St(\mathbf{m}^L)\neq\{e\}} P_{\mathcal{M}^L}(\mathbf{m}^L) \qquad (2)$$

On the other hand, if for some $\mathbf{m}^L, St(\mathbf{m}^L) \neq \{e\}$ holds, then there exists a maximal key τ such that $\mathbf{m}^L \in [F(\tau)]^L$. Therefore we have:

$$\sum_{\mathbf{m}^L:St(\mathbf{m}^L)\neq\{e\}} P_{\mathcal{M}^L}(\mathbf{m}^L) \leq$$

$$\sum_{\tau \in \mathcal{K}_{\max}} \sum_{\mathbf{m}^L \in [F(\tau)]^L} P_{\mathcal{M}^L}(\mathbf{m}^L) =$$

$$\sum_{\tau \in \mathcal{K}_{\max}} (P_\tau)^L \leq |\mathcal{K}_{\max}|R^L \qquad (3)$$

From (2) and (3) substituting in (1), we finally obtain:

$$\log(2)R^L \leq H(\mathcal{K}|\mathbf{M}^L\mathbf{C}^L) \leq \log(|\mathcal{K}|)|\mathcal{K}_{\max}|R^L$$

which is the desired result. ∎

Note that Theorem 2.5 shows the asymptotic tight exponential behaviour of $H(\mathcal{K}|\mathbf{M}^L\mathbf{C}^L)$ with exponent base R equal to the maximum among sums of symbol probabilities of the fixed sets of maximal keys.

III. Applications

We shall consider four applications of Theorem 2.5. For the first two applications we assume without loss of generality that $P_{\mathcal{M}}(1) \geq P_{\mathcal{M}}(2) \geq \ldots \geq P_{\mathcal{M}}(N)$.

1. Let $\mathcal{K} = \mathcal{S}_{\mathcal{M}}$ – the case of simple substitution cipher. Clearly, maximal keys are the transpositions. Therefore, $R_1 = \sum_{j=1}^{N-2} P_{\mathcal{M}}(j) = 1 - P_{\mathcal{M}}(N) - P_{\mathcal{M}}(N-1)$, $|\mathcal{K}| = N!$ and $|\mathcal{K}_{\max}| = \binom{N}{2}$. This result is obtained in [1].

2. let $\mathcal{K} = \mathcal{A}_{\mathcal{M}}$, where $\mathcal{A}_{\mathcal{M}}$ is the alternating group acting on $\mathcal{M}$. It can be easily seen that maximal keys are the substitutions which can be represented as a superposition of cycle of length 3 and disjoint to this cycle identity substitution. Clearly, these substitutions belong to $\mathcal{A}_{\mathcal{M}}^*$. Proceeding as in the previous case we get $R_2 = \sum_{j=1}^{N-3} P_{\mathcal{M}}(j) = 1 - P_{\mathcal{M}}(N) - P_{\mathcal{M}}(N-1) - P_{\mathcal{M}}(N-2)$, $|\mathcal{K}| = N!/2$ and $|\mathcal{K}_{\max}| = \binom{N}{3}$.

3. Let d be a positive integer. We will consider messages of length $L = kd, k \geq 1$. Since the message source is memoryless it is memoryless also over the cartesian product $\mathcal{M}^d$ considered as an alphabet.

Let $\pi \in \mathcal{S}_\Delta$, where $\Delta = \{1, 2, \ldots, d\}$. Define a mapping $T_\pi : \mathcal{M}^d \to \mathcal{M}^d$ as $T_\pi(m_1m_2\ldots m_d) \overset{\text{def}}{=} m_{\pi(1)}m_{\pi(2)}\ldots m_{\pi(d)}$. Since π is a substitution, it follows that T_π is a substitution of $\mathcal{M}^d$. The set $\{T_\pi/\pi \in \mathcal{S}_\Delta\}$ with superposition operation is a group isomorphic to $\mathcal{S}_\Delta$ and it is a subgroup of $\mathcal{S}_{\mathcal{M}^d}$.

Furthermore it is well known that any $\pi \in \mathcal{S}_\Delta^*$ can be represented as a superposition of disjoint cycles in a unique way to the order of multipliers. A partition of Δ corresponds to this representation and it is not dificult to see that the fixed set $F(T_\pi)$ consists of exactly those $\mathbf{m}^d \in \mathcal{M}^d$ whose letters in numbered places belonging to the same subset of the partition of Δ, coincide. Therefore, if we take $\rho \in \mathcal{S}_\Delta^*$ different from π such that the partition of Δ detrmined by ρ is "more detailed", then the inclusion $F(T_\pi) \subset F(T_\rho)$ holds. The latter shows that those T_π are maximal for which π is represented as a superposition of one cycle of length 2 and disjoint to this cycle identity substitution, i.e. π is a transposition.

Taking into account the above considerations it can be easily computed the rate $R_3 = \sum_{j=1}^{N} P_{\mathcal{M}}^2(j)$, the order of subgroup $|\mathcal{K}| = d!$ and the number of the maximal keys $|\mathcal{K}_{\max}| = \binom{d}{2}$

for this case. Finally, we note that inequalities of Theorem 2.5 now become:

$$\log(2)R_3^k \leq H(\mathcal{K}|\mathbf{M}^{kd}\mathbf{C}^{kd}) \leq \log(d!)\binom{d}{2}R_3^k$$

4. Let now, the alphabet $\mathcal{M}$ be a finite field with $|\mathcal{M}| = N$, where N is a power of prime number. Let $\mathcal{K}$ be the group of affine transformations

$$g : y = ax + b; \qquad a, b \in \mathcal{M}, a \neq 0$$

Obviously, each affine transformation $y = ax + b, a \neq 1$ possesses just one fixed point $x_f = b/(1 - a)$ and when b runs through $\mathcal{M}$ the same does x_f. Moreover translations $y = x + b, b \neq 0$ do not possess any fixed points. Thus, we have $R_4 = \max\{P_{\mathcal{M}}(n)/n \in \mathcal{M}\}$, $|\mathcal{K}| = N(N - 1)$ and $|\mathcal{K}_{\max}| = N(N - 2)$.

IV. CONCLUSIONS

Despite that during the past three decades mainly computational aspects of cryptology have been developped, there is still place for information-theoretic investigations. An example in this direction is the theorem from the present paper which justifies mathematically the intuitive understanding that the recovery of the key in known-plaintext attack on substitution ciphers is more difficult when this key possesses many fixed points.

V. ACKNOWLEDGMENT

REFERENCES

[1] Dunham J.G., Bounds on Message Equivocation for Simple Substitution Ciphers, IEEE Trans. Inform. Theory, vol IT-26, pp. 522-527, September 1980.

[2] Shannon C.E., Communication Theory of Secrecy Systems, Bell Syst. Tech. J., vol. 28, pp. 656-715, October 1949.

[3] Hellman M.E., An extension of the Shannon theory approach to cryptography, IEEE Trans. Inform. Theory, vol IT-23, pp. 289-294, May 1977.

[4] Blom R.J., Bounds on key equivocation for simple substitution ciphers, IEEE Trans. Inform. Theory, vol IT-25, pp. 8-18, January 1979.

[5] Sgarro A., Error Probabilities for Simple Substitution Ciphers, IEEE Trans. Inform. Theory, vol IT-29, pp. 190-197, March 1983.

[6] Gallager R., *Information Theory and Reliable Communication*, New York: Wiley, 1968.